IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

Reliable Multi Authority Authentication and Attribute-Based Encryption System for Distributed Data Security

Mrs. S. Yoga[1], Mrs. Kanagavalli[2]

Assistant Professor, Department of Computer Science, Sakthi college of Arts and Science for Women, Oddanchatram[1]

M. Phil Scholar, Department of Computer Science, Sakthi college of Arts and Science for Women, Oddanchatram[2]

Abstract: Data storing and sharing is an imperative functionality in distributed networks. We propose a secure and reliable multi-owner data sharing scheme in cloud environment. It implies that any user in the group can securely share data with others in the distributed systems. The proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners directly. The size and computation overhead of encryption are constant and independent with the number of revoked users.

Keywords: Cloud security, Hybrid Cloud, Attribute Based Encryption, Private Cloud.

I. INTRODUCTION

Cloud computing is a paradigm that allows users to access application residing at distant locations especially data centers. NIST definition (Mell and Grance, 2011) of cloud computing states that "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction".

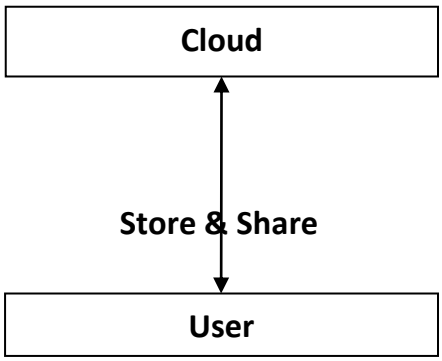

Figure 1.1: Overview of Cloud Computing Paradigm

Fig 1.1 depicts an overview of cloud computing paradigm. Cloud offers vast variety of services in pay-as-you-go manner; in other words it provides services on the basis of utility computing. Amazon Web Services, Google App Engine and Microsoft Azure are some of the current examples of public utility cloud computing services. Amazon Web Services provides a suite of cloud-based services including storage, computation and even human intelligence through the Amazon Mechanical Turk. Further the commercial web service provided by Amazon named Elastic Compute cloud (EC2) allows small companies and individuals to rent computers on which to run their own computer applications. In addition to this Google offers browser-based enterprise applications, through services such as Google Apps. The most important contribution to cloud computing has been the emergence of killer apps from leading technology giants such as Microsoft and Google. As the usage of cloud computing is increasing exponentially, the necessity of providing security and access control has become mandatory.

The primary motivation of our work is the need of security in terms of access control for cloud computing services with multi factor authentication. Several large scale industries and organizations make use of computation solutions and storage infrastructures provided by the cloud service providers (CSP). The affordable and reliable nature of cloud services makes it usage prominent with wider range of organizations. But still the emergence of several security issues by means of attacks and vulnerabilities had created a great scope for security research. The newer ways of using cloud computing for computing, storage and deployment is leading to the development of the cloud domain in different technological perspectives, leading to need of added security. This will motivate the idea of using cloud computing for critical applications.

Privacy preservation and access management forms the two major influences for maintaining cloud data security. The main theme of most of the existing schemes is to make use of cryptographic measures to achieve data security. Each scheme provides solution to specific technical functionality issues, but lags in the provision of complete suitable solution to issues relating to cloud data

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

access management. The reason is the high level complexity of cryptographic techniques. Existing access control techniques are not designed specifically for a certain application, which can match hardware's and effective signatures. The generality will be a hurdle to achieve fine grained access control and other security properties like fast revocation and access control delegation. In this paper, we present an extensive analysis of existing access control schemes with special importance to Attribute Based Encryption techniques. A complete solution to cloud data access problems with appropriate user access provision methods and improved security establishment techniques are presented in this research work.

CONTRIBUTIONS

In this paper we introduce a set of techniques and frameworks to solve some of the major security challenges associated with cloud computing environment. The key contributions of the thesis were enumerated as follows:

MACP-ABE (Multi Authority Cipher Policy based attribute based encryption)

We introduces a new key aggregation scheme which is named as MASS (Mobile Authentic and Secure Sum up) technique, which collects the keys from all owners and creates an aggregated key for data decryption.

Unlike the previous works, the average size and time of rekeying messages have been avoided. So the communication overhead and time factors are considered here.

The proposal develops a three-step scheme for MASS implementation.

The first one is initial key generation for both single owner data and multi owner data group. The first algorithm can generate a key-tree that corresponds to the optimal key-tree obtained by mathematical analysis.

The second step of the mechanism in MASS is an optimal key-tree maintenance and aggregation algorithm for multi owner data.

The second scheme eliminates the existing re-key and key alteration processes.

The third step of the scheme is the Device based authentication scheme, which helps to gather the encrypted keys from the device and aggregates together for decryption.

Finally this performs the crypto process using the aggregated (sum up) key. This technique is named as **MACP-ABE.**

In order to ensure thesis goals with newly proposed solutions, certain properties relating to better access provision were selected and it has been focused throughout the thesis. The chosen properties were considered to be most important in terms of addressing the issues preventing cloud data access vulnerability. The properties were classified into three categories - security, access control and performance.

II. PROBLEM DEFINITION

Page `Data sharing is an important functionality in cloud domain. This is very important in distributed environment to keep the data more secure and vulnerable less. When considering the flexibility and scalability in data sharing, there are numerous issues arises in the field of security. Efficient data encryption and key sharing schemes have been proposed in the literature, even those schemes were not completely secure in the multi owner data sharing environment. For both security and efficiency, a group key which is shared only by a group of users has been employed for access control. A message for the group is encrypted by the group key which is provided by the group manager. The encrypted group key is transmitted only once to the owner of the file.

Then the transmitted message can be decrypted by only group members having the group key. However, the group key is updated whenever the group membership changes for forward and backward secrecy, which can cause a serious problem with rekeying overhead. And key should be created for every file separately. So the communication and key overhead was high. The challenging problem is how to effectively share encrypted data with effective authentication and minimum key generation overhead. The several applications suffer from in efficient key authentication and key management problems.

Transferring the secret keys inherently requires a protected way, and storing these keys requires rather expensive secure storage. The keys should be unique for every owner for a single file. The costs and complexities involved generally increase with the number of the decryption keys to be shared. The problem occurs when the user try to send the decrypted keys to the unknown multiple users. The user who receives the key need to combine with their group key which is provided by the group manager. The group manager is common to the entire user in the particular group. However the user who sends the encrypted message with their group key only allowed receiving the file.

III. PROPOSED SYSTEM

In modern cryptography, a fundamental problem the literature often says is about leveraging the secrecy of a small piece of knowledge into the ability to perform cryptographic functions which is sampled as encryption and authentication multiple times. In this research, this introduces the concept of how to make a decryption key more powerful and authentication is reliable in the sense that it allows decryption of multiple cipher texts, without increasing its size. The followings are the major contribution of the proposed system. The research work introduces a set of techniques and frameworks to solve some of the major security challenges associated with cloud computing environment. The key contributions of the thesis were enumerated as follows.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

1. A novel scheme called MACP- ABE scheme collective advancement on access control and authentication scheme for multi authority cloud storage systems for preventing numerous security breaks and violations which occurs in the hybrid cloud environment.
2. the research introduce a novel cryptographic access control technique named as **M_Key Cryptography** that provides fine-grained data access and storage correctness verification to data users through the use of the dynamic token granting system.
3. To enable seamless, dynamic and secure interaction of cloud services over larger activity, the research design and implement a **MASS(Mobile Authentic and Secure Sum up)** and hardware authentication scheme that solves the problem of user attribute revocation with forward and backward security assurance.
4. This presents a novel ABE scheme that preserves the property of security and privacy over outsourced sensitive information. It is achieved through the process of key aggregation techniques.
5. A new Device based authentication scheme is introduced to avoid key guessing and stealing issues, and this helps to gather the encrypted keys from the device and aggregates together for decryption.
6. A hardware based authentication scheme is additionally proposed to increase the security of the data. This matches the MAC and IP based signatures while decrypting.

In order to ensure thesis goals with newly proposed solutions, certain properties relating to better access provision were selected and it has been focused throughout the thesis. The chosen properties were considered to be most important in terms of addressing the issues preventing cloud data access vulnerability. The properties were classified into three categories - security, access control and performance.

IV. MACP-ABE

MACP-ABE section introduces the process and steps of the proposed system. the MACP-ABE scheme includes different steps and iterations of authentication, which as summarized into three categories.

The following are the steps involved in the proposed system.

1. Key setup and Key generation phase
2. Cryptographic phase
3. Device authentication phase

A. Key Aggregation

Key aggregation chapter introduces a new key aggregation scheme which is named as **MASS** technique, which collects the keys from different sources and creates an aggregated key for data decryption. Unlike the previous works, the average size and time of rekeying messages have been avoided. So the communication overhead and time factors are considered here.

B. The proposal develops a three-step scheme for MACP-ABE implementation.

The first one is initial key generation for both single owner data and multi owner data group. The first algorithm can generate a key-tree that corresponds to the optimal key-tree obtained by mathematical analysis.
The second step of the mechanism in MACP-ABE is an optimal key-tree maintenance and aggregation algorithm for multi owner data.
The second scheme eliminates the existing re-key and key alteration processes.
The third step of the scheme is the Device based authentication scheme, which helps to gather the encrypted keys from the device and aggregates together for decryption.
Finally this performs the crypto process using the aggregated (sum up) key. This technique is named as **M_Key Cryptography (M_KC).** The M_Key is referred the proposed MACP-ABE scheme which is mentioned above.
In **M_KC**, users encrypt a message not only under a public-key, but also under an adjunct of cipher text called class. That means the cipher-texts are further categorized into different classes.

C. Key Distribution

The key owner holds a master-secret called master-secret key, which can be used to extract secret keys for different classes. More importantly, the extracted key can have an aggregate key which is as compressed as a secret key for a single class, but aggregates the power of many such keys, i.e., the decryption power for any subset of cipher-text classes.

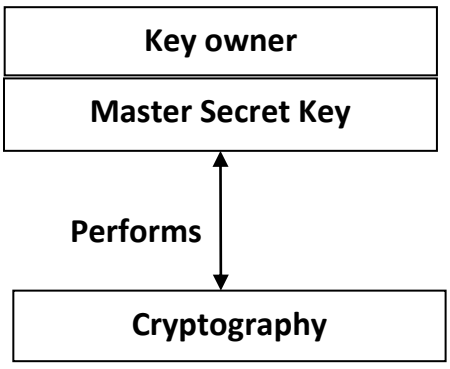

Fig 1.0 key generation process

With the proposed solution, the owners can simply send their private keys via a secure SMS along with the encrypted message. The system will collect and aggregate the keys together. This aggregated key will be used to decrypt the encrypted data's. The sizes of cipher-text, public-key, and master-secret key and aggregate key in the M_KC schemes are all of constant size. Prior outcomes may achieve a similar property featuring a constant-size decryption key, but the classes need to receive the aggregated key via email. The proposed work is flexible in the sense that this constraint is eliminated, that is, no

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

special relation is required between the classes. All creations can be proven secure in the standard model. To the best of our knowledge, the proposed Mass based aggregation M_KC has not been implemented earlier.

V. RESULTS AND ANALYSIS

A. Implementation Configuration

The implementation is carried out using dotnet cloud framework.. The Cloud model uses the random client generation model. There are 5 clients defined in an implementation with unique identity.

Performance results:

The performance of our proposed work MACP using ABE node scheme is compared with the existing approach ABE. This considered the key size selection on the ABE is compared at the time of verification.

Table 1.0 Encryption Time comparison table

Parameters	Existing (ABE)	Proposed (MACP ABE)
Datasize(512)	8	3
Datasize(1024)	18	7

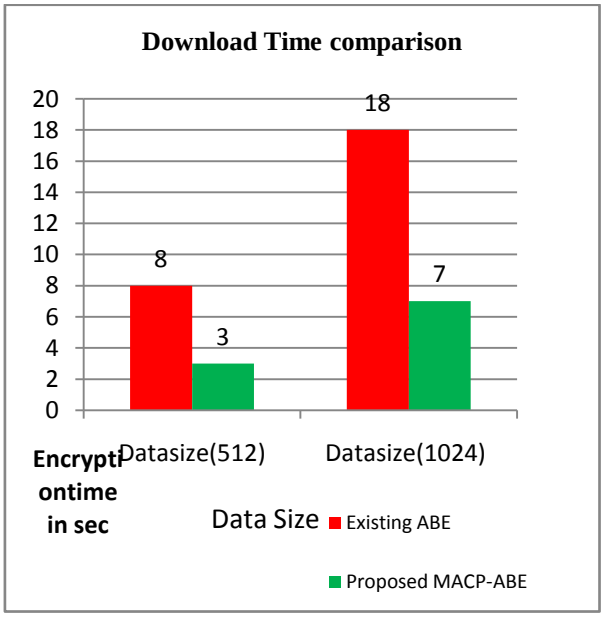

Fig 4.0 comparison chart

Fig. 2.0 presents the encryption overhead costs for different size of data's. The X axis represents the data size, while the Y axis represents the time for encryption. The MACP-ABE compared with the existing ABE method in the form of attribute based encryption.

VI. CONCLUSION

In this paper, a new framework for Cloud data security is proposed, that is named as MACP-ABE .It uses different algorithms and techniques to secure cloud data. With the help of ABE schemes and other device based authentication MACP-ABE effectively secure data in the cloud environment. The major advantage of the system is that, if a user shares a data in the cloud, the data will be more secure than ever.

REFERENCES

[1] H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Trans. Services Computing, vol. 6, no. 4, pp. 551-559, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6357181, Oct.-Dec. 2012.
[2] Wang, S.S.M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," Proc. IEEE 33rd Int'l Conf. Distributed Computing Systems (ICDCS), 2013.
[3] Title: A Break in the Clouds: Towards a Cloud Definition Author: Luis M. Vaquero, Luis Rodero-Merino, Juan Caceres, Maik Lindner Telefonica Investigacion y Desarrollo and SAP Research Madrid, Spain, EU and Belfast, UK, EU
[4] S.S.M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R.H. Deng, "Dynamic Secure Cloud Storage with Provenance," Cryptography and Security, pp. 442-464, Springer, 2012.
[5] M.J. Atallah, M. Blanton, N. Fazio, and K.B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Trans. Information and System Security, vol. 12, no. 3, pp. 18:1-18:43, 2009.
[6] Chu, C., et al. "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage." (2014): 1-1.
[7] Kallahalla, Mahesh, et al. "Plutus: Scalable Secure File Sharing on Untrusted Storage." Fast. Vol. 3. 2003.
[8] Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.
[9] Liu, Xuefeng, et al. "Mona: secure multi-owner data sharing for dynamic groups in the cloud." Parallel and Distributed Systems, IEEE Transactions on 24.6 (2013): 1182-1191.
[10] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010

BIOGRAPHIES

Mrs. S. Yoga completed MSc (CS&IT) Madurai Kamaraj University. She working as assistant professor of computer science department, sakthi arts and Science College, oddanchatram. Her Teaching experience 4 years. Her area of interest Network Security

Mrs. Kanagavalli completed MSc and currently pursing M.phil computer science at sakthi Arts and science college oddanchatram. Her teaching experience 1years. Her area of interest Network Security.